PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-342862
(43)Date of publication of application : 29.11.2002

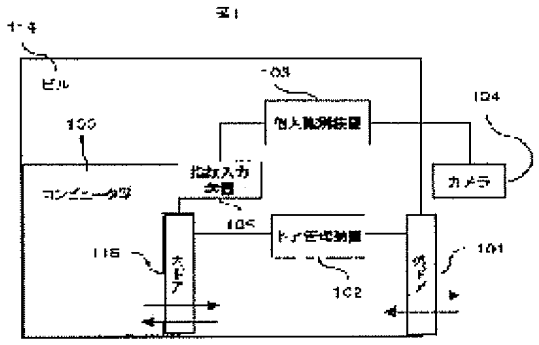
(51)Int.Cl. G08B 25/04
E05B 49/00
G06T 7/00

(21)Application number : 2001-145785
(22)Date of filing : 16.05.2001

(71)Applicant : HITACHI LTD
(72)Inventor : MIMURA MASAHIRO
SETO YOICHI
MURATA KAZUYOSHI

(54) ACCESS CONTROL SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To improve the resistance to forgery of organism information, the acceptability of a user, a collation time, the accuracy, and a system construction cost of an identification system using the user's inherent organism information.
SOLUTION: A face of a person entering into a building 114 is photographed by a camera 104. When the picture is agreed with a person registered in advance, a personal identification device 103 records the personal ID, a result of collation, and the entry date and time as logs, and outputs a command for unlocking a door of the building 114. A fingerprint input device 104 acquires the fingerprint of the person entering into a computer room 100 in the building 114. The personal identification device 103 collates the acquired fingerprint with the characteristic amount of the recorded registered fingerprint of the person who is about to enter. Further the entitlement of the person entering in the room is comprehensively determined on the basis of a result of the collation of the face of the person entering in the room and a result of the collation of the fingerprint. When the person is entitled to enter, the command for unlocking the door of the computer room 100 is outputted.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－342862
（P2002－342862A）
(43)公開日　平成14年11月29日(2002.11.29)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０８Ｂ　25/04		Ｇ０８Ｂ　25/04	Ｆ	２Ｅ２５０
Ｅ０５Ｂ　49/00		Ｅ０５Ｂ　49/00	Ｒ	５Ｂ０４３
Ｇ０６Ｔ　7/00	５１０	Ｇ０６Ｔ　7/00	５１０Ａ	５Ｃ０８７

審査請求　未請求　請求項の数10　ＯＬ　（全 13 頁）

(21)出願番号　特願2001－145785(P2001－145785)

(22)出願日　平成13年５月16日(2001.5.16)

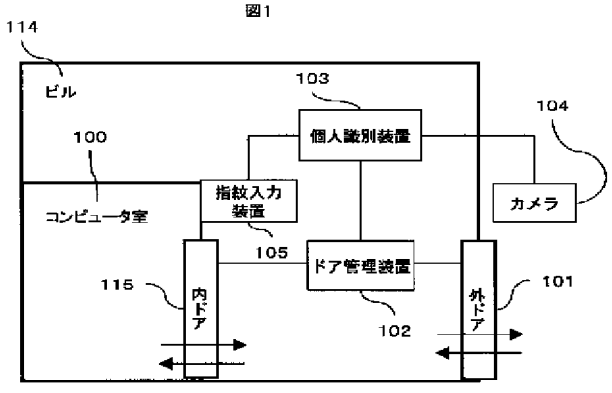
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　三村　昌弘
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　瀬戸　洋一
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(74)代理人　100075096
弁理士　作田　康夫

最終頁に続く

(54)【発明の名称】　アクセス管理システム

(57)【要約】
【課題】利用者固有の生体情報を用いた本人確認システムの，生体情報の偽造耐性，利用者の受容性，照合時間，精度，システム構築コストを改善する。
【解決手段】ビル114に入ろうとする者の顔をカメラ104で撮影する。あらかじめ登録された者と一致していた場合，個人識別装置103は，個人ID，照合結果，入場日時をログとして記録した後，ビル114のドアの開錠命令を出す。ビル114内のコンピュータ室100に入ろうとする者の指紋を，指紋入力装置104で取得する。個人識別装置103は記録されている入場中の者の登録された指紋の特徴量と取得した指紋を照合する。さらに入場中の者の顔照合結果と指紋照合結果から総合的に立ち入ろうとする者の資格を判定する。資格を持つ者である場合，コンピュータ室100のドアの開錠命令を出す。

図1



1

【特許請求の範囲】

【請求項１】多重にアクセス制御を行うアクセス管理システムであって，第1のアクセスの許可を得ようとする者の，第1の種類の生体情報を取得し出力する，第1の種類の生体情報取得装置と，第2のアクセスの許可を得ようとする者の，第2の種類の生体情報を取得し出力する，第2の種類の生体情報取得装置と，第1のアクセス，第2のアクセスの可否を判定する個人認識装置と，上記個人認識装置の判定結果に従い，第1のアクセスを制御する装置と，上記個人認識装置の判定結果に従い，第2のアクセスを制御する装置と，を備え，上記個人認識装置は，第1のアクセスが許可されている者について，記憶装置が記憶している第1の種類の生体情報と，第1の種類の生体情報取得装置が出力した，第1のアクセスの許可を得ようとする者の上記第1の種類の生体情報とを照合する第1の照合処理部と，上記第1の照合処理部による照合結果を用いて，上記第1のアクセスの許可を得ようとする者によるアクセスの可否を判定する第1の判定処理部と，第1の判定処理部がアクセスを許可した者について，記憶装置が記憶している第2の種類の生体情報と，第2の種類の生体情報取得装置が出力した，上記第1のアクセス中に第2のアクセスの許可を得ようとする者の上記第2の種類の生体情報と照合する第2の照合処理部と，上記第2の照合処理部による照合結果を用いて，上記第2のアクセスの許可を得ようとする者によるアクセスの可否を判定する第2の判定処理部と，上記第1の判定処理部による判定結果を上記第1のアクセスを制御する装置へ通知し，上記第2の判定処理部による判定結果を上記第2のアクセスを制御する装置へ通知するアクセス管理処理部と，を備えることを特徴とするアクセス管理システム。

【請求項２】請求項1に記載のアクセス管理システムであって，前記第2の判定処理部は，上記第1の照合処理部による照合結果と，上記第2の照合処理部による照合結果とを，あらかじめ定めた判定基準に従い，上記アクセス可否を判定することを特徴とするアクセス管理システム。

【請求項３】請求項1に記載のアクセス管理システムであって，上記アクセス管理処理部は，上記第1の判定処理部がアクセスを許可した者の内，上記第1の生体情報が取得されてから上記第2の生体情報が取得されるまでの時間が所定の値以内である者を上記第2の照合処理部が照合対象とするように，上記第1の判定処理部を制御することを特徴とするアクセス管理システム

【請求項４】請求項1に記載のアクセス管理システムであって，上記アクセス管理処理部は，上記第1の判定処理部がアクセスを許可した者の内，上記第2のアクセス許可を得ようとする者の識別情報を用いて，照合の対象となる者を選抜するように，上記第2の照合処理部を制御することを特徴とするアクセス管理システム

2

【請求項５】請求項4に記載のアクセス管理システムであって，第1のアクセスの許可を得ようとする者の，第2の種類の生体情報を取得し出力する，第3の種類の生体情報取得装置をさらに備え，上記第1の照合処理部は，第1のアクセスが許可を得ようとする者について，第2の種類の生体情報を上記記憶装置に記憶させ，上記第2の照合処理部は，上記第1の照合処理部が記憶させた第2の種類の生体情報を照合に用いることを特徴とするアクセス管理システム

【請求項６】請求項1に記載のアクセス管理システムであって，第1の種類の生体情報を取得する装置または第2の種類の生体情報を取得する装置は，アクセスの許可を得ようとする者を赤外線で照射する装置と，上記赤外線照射処理部との位置関係が変化することがない，上記アクセスの許可を得ようとする者の身体の一部の赤外線画像を取得する装置とを有し，上記個人認識装置は，上記赤外線画像を可視画像に変換する処理部を備え，上記第1または第2の照合処理部は，上記変換された可視画像を用いて上記照合を行うことを特徴としたアクセス管理システム。

【請求項７】請求項1に記載のアクセス管理システムであって，上記アクセスとは，物理的領域への立ち入りまたは情報システムの利用であることを特徴とするアクセス管理システム。

【請求項８】請求項1に記載のアクセス管理システムであって，上記生体情報とは，顔画像または指紋のいずれかであることを特徴とするアクセス管理システム。

【請求項９】アクセス管理システムに用いる個人認識装置であって，第1のアクセスが許可されている者について，記憶装置が記憶している第1の種類の生体情報と，第1のアクセスの許可を得ようとする者の上記第1の種類の生体情報とを照合する第1の照合処理部と，上記第1の照合処理部による照合結果を用いて，上記第1のアクセスの許可を得ようとする者によるアクセスの可否を判定する第1の判定処理部と，第1の判定処理部がアクセスを許可した者について，記憶装置が記憶している第2の種類の生体情報と，上記第1のアクセス中に第2のアクセスの許可を得ようとする者の上記第2の種類の生体情報と照合する第2の照合処理部と，上記第2の照合処理部による照合結果を用いて，上記第2のアクセスの許可を得ようとする者によるアクセスの可否を判定する第2の判定処理部と，上記第1の判定処理部による判定結果を上記第1のアクセスを制御する装置へ，上記第2の判定処理部による判定結果を上記第2のアクセスを制御する装置へ，それぞれへ通知するアクセス管理処理部と，からなることを特徴とする個人認識装置。

【請求項１０】計算機を，アクセス管理システムに用いる個人認識装置として処理させるためのプログラムであって，第1のアクセスが許可されている者について，記憶装置が記憶している第1の種類の生体情報と，第1のア

クセスの許可を得ようとする者の上記第1の種類の生体情報とを照合する第1の照合処理部を具現化するプログラムコードと，上記第1の照合処理部による照合結果を用いて，上記第1のアクセスの許可を得ようとする者によるアクセスの可否を判定する第1の判定処理部を具現化するプログラムコードと，第1の判定処理部がアクセスを許可した者について，記憶装置が記憶している第2の種類の生体情報と，上記第1のアクセス中に第2のアクセスの許可を得ようとする者の上記第2の種類の生体情報と照合する第2の照合処理部を具現化するプログラムコードと，上記第2の照合処理部による照合結果を用いて，上記第2のアクセスの許可を得ようとする者によるアクセスの可否を判定する第2の判定処理部を具現化するプログラムコードと，上記第1の判定処理部による判定結果を上記第1のアクセスを制御する装置へ，上記第2の判定処理部による判定結果を上記第2のアクセスを制御する装置へ，それぞれへ通知するアクセス管理処理部を具現化するプログラムコードと，からなることを特徴とする個人認識プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は，あらかじめ資格を与えた利用者にアクセスを許可するアクセス管理技術に関する。

【０００２】

【従来の技術】アクセス管理技術に関連する公知例として以下のものがある。

（1）指紋による入退室管理システム

特開平11−053666号公報に記載されているように，利用者の指紋を用いて管理領域への入退室を管理するシステムであって，利用者の指紋から抽出した特徴量をあらかじめ登録しておき，利用者が管理領域へ入場する際に，あらかじめ登録した指紋の特徴量とあらたに入力した指紋画像の照合を行うことで，利用者が入場を許可されていることを確認し，管理領域への入場を可能とする。

（2）顔および指紋によるマルチモーダル本人認証システム

"Biometrics," A. Jain他，Kluwer Academic Publishers，1999，pp327−344に記述されているように，利用者の顔と指紋の2種類の生体情報の特徴量をあらかじめ登録しておき，本人確認を要求する利用者の顔と指紋をそれぞれの特徴量と照合した結果から総合的に本人の確認を行う。

【０００３】

【発明が解決しようとする課題】公知例（1）の方法では，以下の2点が課題となる。

・単一の生体情報に基づいて本人確認を行うため，システムが要求する本人確認の精度（本人拒否率および他人受入率）を満たせない可能性がある。

・単一の生体情報に基づいて本人確認を行うため，生体情報の偽造に対する耐性が弱く，なりすましによる不正な入場を防止できない可能性がある。

【０００４】公知例（2）の方法を公知例（1）の指紋に代わって用いる場合では，複数の生体情報を用いることで上記2点の課題に対応することができるが，以下の3点が課題となる。

・複数の生体情報を用いて本人確認を行うため，セキュリティが必要以上に強固となる場合があり，利用者の利便性が低下する。また，システム構築コストが増大する。

・利用者を識別する際に，複数の登録者全員を複数の生体情報の照合の対象とするため，計算時間が増加する。

・顔画像を，照明光，自然光などすでに在る可視光の光源を用いて取得するため，光源の位置が一定せず，同じ顔から得られた画像が大きく変化し，その結果認識精度が劣化する。

以上を改善したアクセス管理システムまたはそのための個人認識装置が望まれている。

【０００５】

【課題を解決するための手段】本発明は，必要な本人確認の精度を満たし，かつ生体情報の偽造に対する高い耐性を持ち，なりすましによる不正なアクセスを防止できる，アクセス管理システムまたはそのための個人認識装置を提供する。

【０００６】また，本発明は，要求されるセキュリティレベルに応じた，適正なアクセスコントロールを行い，高い利便性，低いシステム構築コスト，短い計算時間を実現できるアクセス管理システムまたはそのための個人認識装置を提供する。

【０００７】本発明の一態様によれば，本発明のアクセス管理システムは，多重にアクセス制御を行うアクセス管理システムであって，第1のアクセスの許可を得ようとする者の，第1の種類の生体情報を取得し出力する，第1の種類の生体情報取得装置と，第2のアクセスの許可を得ようとする者の，第2の種類の生体情報を取得し出力する，第2の種類の生体情報取得装置と，第1のアクセス，第2のアクセスの可否を判定する個人認識装置と，上記個人認識装置の判定結果に従い，第1のアクセスを制御する装置と，上記個人認識装置の判定結果に従い，第2のアクセスを制御する装置と，を備える。

【０００８】上記個人認識装置は，第1のアクセスが許可されている者について，記憶装置が記憶している第1の種類の生体情報と，第1の種類の生体情報取得装置が出力した，第1のアクセスの許可を得ようとする者の上記第1の種類の生体情報とを照合する第1の照合処理部と，上記第1の照合処理部による照合結果を用いて，上記第1のアクセスの許可を得ようとする者によるアクセスの可否を判定する第1の判定処理部と，第1の判定処理部がアクセスを許可した者について，記憶装置が記憶している第2の種類の生体情報と，第2の種類の生体情報取

得装置が出力した，上記第1のアクセス中に第2のアクセスの許可を得ようとする者の上記第2の種類の生体情報と照合する第2の照合処理部と，上記第2の照合処理部による照合結果を用いて，上記第2のアクセスの許可を得ようとする者によるアクセスの可否を判定する第2の判定処理部と，上記第1の判定処理部による判定結果を上記第1のアクセスを制御する装置へ通知し，上記第2の判定処理部による判定結果を上記第2のアクセスを制御する装置へ通知するアクセス管理処理部と，を備える。

【０００９】さらに，他の態様によれば，上記第2の判定処理部は，上記第1の照合処理部による照合結果と，上記第2の照合処理部による照合結果とを，あらかじめ定めた判定基準に従い，上記アクセス可否を判定してもよい。本発明におけるアクセスとは，対象となるものへの立ち入り，または対象となるものを利用すること，を意味する。たとえば，前者は，制限領域へ立ち入ることを指し，後者は，情報システムの利用することを指す。また，本発明は，アクセス制限領域内へのアクセスを開始した日時から一定時間が経過した場合に当該アクセス者の記録を削除する機能とを有してもよい。上記第1のアクセス制限領域内には，第2，第3のアクセス制限領域を設け，それぞれが異なる生体情報によるアクセス制限を行っても良い。なお，同じ種類の生体情報であっても，情報源が異なれば異なる種類の生体情報として利用できる。具体的には，同じ指紋情報であっても，異なる指であれば異なる生体情報として利用できる。また本発明は，より高いセキュリティレベルを要求される管理領域には，他の生体情報を用いたアクセス制御を併用することで，セキュリティレベルにあった，適正なアクセス制御を行い，高い利便性および低いシステム構築コストを実現することができる。

【００１０】また，本発明は，個人識別装置において，識別対象者を赤外光で照らし，その反射である赤外線画像を取得する機能を有し，さらに上記赤外光の光源と画像を取得する機能との位置関係を一定に保つことにより，可視光の光源の位置に影響されることなく高精度な個人識別を行うことができる。識別精度をより高めるために，可視光をカットするフィルタを併用しても良い。

【００１１】

【発明の実施の形態】第1の実施の形態として，入場が制限されたビルにおいて，さらに高いセキュリティが必要とされるコンピュータ室への入場管理を例に説明する。本実施例では，個人識別に用いる生体情報として利用者の顔と指紋を用いる。ただし，顔と指紋に限定するものではなく，他の生体情報を用いることも可能である。本実施例における指紋の入力，登録，照合は特開平10–149446号公報に記載された方法などを用いればよい。また本実施例における顔の入力，登録，照合は特開2000–132675号公報に記載された方法などを用いればよい。

【００１２】図1は第1の実施例の概略を説明する図である。本実施例は，あらかじめ許可された者のみが入場可能なビル114，そのドア101，ビル114内でさらに高いセキュリティが要求されるコンピュータ室100，そのドア115，ドア101およびドア115の開錠，施錠を行うドア管理装置102，入場しようとする者があらかじめ入場を許可されているかどうかを判定する個人識別装置103を設置する。個人識別装置103には，ビル114に入場しようとする者の顔画像を取得するカメラ104，コンピュータ室100に入場しようとする者の指紋を取得する指紋入力装置105が接続される。

【００１３】ビル114に入場しようとする者は，カメラ104にて顔画像を入力する。個人識別装置103はあらかじめ登録された個人の顔の特徴量と新たに入力された顔画像を照合し，あらかじめ登録された個人であると判定した場合，個人ID，照合結果である類似度，入場日時をログとして記録した後，ドア管理装置102にドア101の開錠命令を出す。ドア管理装置102は開錠命令を受けてドア101を開錠する。　ビル114内のコンピュータ室100に入場しようとする者は，指紋入力装置105にて指紋を入力する。個人識別装置103はログが記録した入場者のうち，ビルに入場した日時からの経過時間が一定時間以下であるものについて，入力された指紋と，あらかじめ登録された指紋の特徴量とを照合する。さらに個人識別装置103は，ログが記録した入場者の顔照合の結果である類似度と指紋の照合結果である類似度とから総合的に個人を特定する。個人識別装置103は，個人が特定できた場合，ドア管理装置102にドア115の開錠命令を出す。ドア管理装置102は開錠命令を受けてドア115を開錠する。

【００１４】以下本実施例を詳細に説明する。図2に個人識別装置103の機能構成例を示す。個人識別装置103は以下に示す機能から構成する。すなわち，ビルへ入場しようとする者の顔画像を得るカメラ104と顔画像入力機能211，ビルへの入場を許可された者の顔の特徴量をあらかじめ保持しておく顔の特徴量データベース201，顔画像と顔の特徴量を照合し，両者の類似度を出力する顔照合機能213，顔の類似度に基づき個人を特定し，個人IDと類似度を出力する顔判定機能217，コンピュータ室100へ入場しようとする者の指紋画像を得る指紋入力装置105と指紋入力機能212，コンピュータ室100への入場を許可された者の指紋の特徴量をあらかじめ保持しておく指紋の特徴量データベース203，指紋画像と指紋の特徴量を照合し，両者の類似度と新たに入力した指紋画像の照合を行い，両者の類似度を出力する指紋照合機能214，顔照合機能213および指紋照合機能214から得た類似度と判定基準データ204を用いてコンピュータ室100へ入場しようとする者を特定し，個人IDを出力する融合判定機能216，顔判定機能217あるいは融合判定機能216が出力した個人IDなどを受けて，アクセスログ202を更新し，ドア管理装置102に開錠命令を出力する入場者管理機能215

から成る。本実施例では，特徴量データベースは個人識別装置内に設置されているが実際にはこの限りではなく，ビル114外に設置してネットワークで接続することも可能である。

【００１５】個人識別装置103は，図18に示すように，CPU1801とメモリ1802と固定記憶装置1803と外部インタフェース1804とを備える一般的な計算機を用いて実現することができる。さらに，個人識別装置103を構成するそれぞれの機能(処理部ともいう)は，上記計算機においてCPU1801が固定記憶装置1803に格納されているプログラムをメモリ1802上に実行することにより具現化できる。各プログラムは，FD，CDROMなどの外部記憶装置またはインターネットなどのネットワーク1805から，上記外部インタフェース1804を介して固定記憶装置1803またはメモリ1802に導入されてもよい。カメラ104，指紋入力装置105，ドア管理装置102は，上記外部インタフェース1804に接続される。

【００１６】図3はビルへの入場を許可された者の顔の特徴量データベース201を例示する。データベースには個人のIDおよび顔の特徴量を関連付けて保存する。個人IDは全ての個人に対してユニークであればどんなものでもよい。また本実施例ではあらかじめ10人がビルへの入場を許可されているものとしているが，この限りではない。図4はコンピュータ室100への入場を許可された者の指紋の特徴量データベース203を例示する。データベースには個人IDおよび指紋のテンプレートを関連付けて保存する。個人IDは全ての個人に対してユニークであればどんなものでもよい。また本実施例ではビルへの入場を許可された10人のうち7人がコンピュータ室100への入場を許可されているものとしているが，この限りではない。また本例では一人に対して1つの指紋を登録しているが，複数の指紋を登録してもよい。図5は判定基準データ204の例である。本例では，類似度に作用させる係数，および係数を作用させた後の値に対して本人であるかどうかを判定するためのしきい値を記録している。判定基準の方法および判定基準データは本例に限定しない。図6はアクセスログ202の例である。本例では，ある者について，ビルに入場した日時，その個人IDおよび顔照合の結果の類似度を記録している。本図は3人が入場している場合の例を示している。

【００１７】図7は本実施例のビルへの入場管理の概略フローを示す。

ステップ705：顔画像入力機能211が，入場しようとする者の顔画像を取り込み，特徴量を抽出する。

ステップ710：顔照合機能213が，顔の特徴量データベース201に登録されている各個人の特徴量と，取り込んだ顔画像を照合し，照合した結果（類似度）と個人IDを関連付け，これらを一時的に記憶する。

ステップ715：類似度から顔画像と一致する者の特定を試みる。すなわち，顔判定機能217が，一時的に記憶した類似度の値を用いて，入場しようとする者がどの個人IDに対応するかを判定する。例えば，全ての類似度中最も大きな値を持つものが，あらかじめ設定したしきい値を超えている場合，この類似度を持つ個人IDが入場しようとする者と特定する。しきい値を超えていない場合，入場しようとする者は特定できなかったものとする。

ステップ720：ステップ715の結果に従い，入場しようとする者を特定できた場合はステップ725へ，できなかった場合は処理を終了する。

ステップ725：顔判定機能217が，特定した者の個人IDおよびその類似度を入場者管理機能215に送信する。

ステップ730：入場者管理機能215が，送信されてきた個人IDおよび類似度に日時を付加してアクセスログ202に記録する。既にアクセスログ202に同じ個人IDが存在する場合は，この類似度と日時を更新し，個人IDが存在しない場合には追加する。

ステップ735：入場者管理機能215がビル114の外ドア101を開錠するよう，ドア管理装置102に開錠命令を送信する。

ステップ740：ドア管理装置が，入場者管理機能215から送信されてきた命令に従い，ビル114の外ドア101を開錠する。

【００１８】図8に本実施例のコンピュータ室100への入場管理の概略フローを示す。

ステップ805：指紋入力機能212が，コンピュータ室100に入場しようとする者の指紋画像を取り込み特徴量を抽出する。抽出した特徴量を指紋照合機能214に渡す。

ステップ810：指紋照合機能214が，ビル114へすでに入場している者の個人IDおよび顔照合の類似度を，入場者管理機能215に要求する。入場者管理機能215は，アクセスログ202に記載されたすでに入場している者の入場の日時と現在の日時を比較し，あらかじめ定めた時間以上経過している場合は，その個人IDをアクセスログ202から削除する。この結果残った個人IDとそれに関連づけられた，入場したときの顔照合の類似度を，指紋照合機能214に回答する。

ステップ813：入場者が一人もいなければ処理を終了し，入場者がいれば処理を継続する。

ステップ815：指紋照合機能214が，指紋特徴量データベース203に登録されている者のうち入場者管理機能215から回答された，ビル114にすでに入場している者の指紋の特徴量と，取り込んだ指紋画像とを照合する。さらに照合した者のID，指紋画像を照合した結果の類似度，および顔画像を照合した類似度を融合判定機能216に渡す。このデータは例えば図9のように記述すればよい。個人IDがA010の者はコンピュータ室100に入場を許可されておらず，指紋が登録されていないため，図9のデータに記載されていない。

ステップ817：融合判定機能216が，指紋照合機能214からビルに入場している者の顔照合による類似度と，指紋

照合による類似度のデータを受け取る。さらに，渡された類似度データと判定基準データ204を用いて，入場しようとする者がどの個人IDに対応するかを判定する。例えば，各個人IDにおける指紋照合の類似度に判定基準データの指紋照合の類似度の係数を，顔照合の類似度に顔照合の類似度の係数を掛け，両者の和をとったものを融合判定の評価値とすればよい。

【００１９】図10に融合判定の評価値の例を示す。図5に従い，顔の類似度の係数を0.8，指紋の類似度の係数を1.2として算出した。最大の類似度を持つもの評価値が，あらかじめ設定したしきい値を超えている場合，この類似度を持つ個人IDが入場しようとする者と特定する。しきい値を超えていない場合，入場しようとする者に対応する個人は特定できなかったものとする。

ステップ820：ステップ817の結果に従い，特定できた場合はステップ825へ，できなかった場合は処理を終了する。

ステップ825：特定した者の個人IDと類似度を入場者管理機能215に送信する。

ステップ835：入場者管理機能215がコンピュータ室100のドア115を開錠するよう，ドア管理装置102に開錠命令を送信する。

ステップ840：ドア管理装置102が，入場者管理機能215から送信されてきた命令に従い，コンピュータ室100のドア115を開錠する。

【００２０】上記実施例においては，入場者管理機能215が，アクセスログ202に記載されている，第1のアクセス中の者（ビル114へ入場している者）がアクセスを開始した日時と現在の日時を比較することにより，第2のアクセス（コンピュータ室への入場）に際して照合の対象となる者を選別している。本実施例においては，顔画像を用いるよりも高い判定精度が得られる指紋をより高いセキュリティを必要とする領域へのアクセス管理に使用することで，より確実なセキュリティ管理が可能になる。上記実施例においては，前記のステップ810で説明したように，ある者がビルに入場した時刻からの経過時間があらかじめ定めた値以下であれば，その者は現在もビルに入場中であると判定している。この代替案として，入場した者がビルを退出する際に，顔識別によって再び個人を特定し，退出した者をアクセスログから削除することで，入場中の者を特定する方法も用いても良い。この方法を経過時間による方法と併用しても良い。

【００２１】上記ステップ705の利用者の顔画像の取得の代替案を以下に示す。図11に図2における顔画像入力機能211の詳細な機能構成を示す。図11に示す顔画像入力機能211は，顔に赤外光を照射する赤外線ライト1103，顔から反射してきた赤外光のみを取得する赤外線カメラ，および可視光による顔画像の照合を行う顔照合機能213に接続される。このとき赤外線カメラ1102と赤外線ライト1103との相対位置は固定されており，両者の幾何的関係は常に同じである。また顔画像入力機能211は，赤外線カメラ1102および赤外線ライト1103を制御する画像入力機能1104，顔の赤外線画像を可視光画像に変換する画像変換機能1105，および赤外線画像を可視光画像に変換する際に用いられる輝度変換テーブル1106からなる。図12に輝度変換テーブル1106の例を示す。図12では，赤外線画像の輝度と可視光画像の輝度との関係を保持している。輝度変換テーブル1106の内容は，人間の顔の皮膚の可視光および赤外光に対する反射率などをそれぞれ実験的に求めることによって算出することができる。

【００２２】図13に赤外光を用いた顔照合のフローを示す。

ステップ1305：画像入力機能1104が，赤外線カメラを用いて，入場しようとする者の顔を赤外線で照射する。赤外線の照射は常時行ってもよいが，顔撮影のタイミングを外部から指示される場合は，これに従って短い時間だけ照射することも可能である。

ステップ1310：画像入力機能1104が，赤外線の照射と連動して入場しようとする者の顔の赤外線画像を取り込む。また取り込んだ赤外線画像を画像変換機能1105に渡す。

ステップ1315：画像変換機能1105が，輝度変換テーブルを用いて者の顔の赤外線画像を可視光画像に変換する。本実施例では，赤外線画像の輝度を，輝度変換テーブルに従って変更することで，可視光画像への変換を行っている。可視光画像は顔照合機能213に渡される。

ステップ1320：顔照合機能213が可視光画像を用いて照合する。

【００２３】本実施例では輝度変換テーブルを用いて赤外線画像を可視光画像に変換しているが，例えば，赤外線画像の輝度の関数として可視光画像の輝度を与えることでも，同様の変換を行うことができる。以上説明したように，利用者を赤外線で照射する装置と，利用者の赤外線画像を取得する装置とを常に一定の位置関係に設置し，かつ赤外線画像を可視光による画像に変換することで，可視光による光源の強度，位置の影響を受けることなく高精度な照合を行うことができる。

【００２４】本実施例では，入場が制限されたビル内にあるさらに安全性を要求されるコンピュータ室100への入場管理を説明しているがこの限りではない。例えば第2の実施例で述べるように，入場を管理されたビル内の情報システムへのアクセス管理などに適用することもできる。

【００２５】第2の実施例として，入場が制限されたオフィス内の端末へのアクセス(ログイン)を制限するシステムを説明する。図14は第2実施例の概略を説明する図である。本実施例は，あらかじめ許可された者のみが入場可能なオフィス1400，そのドア101，ドア101の開閉を行うドア管理装置102，入場しようとする者および端末1

408にログインしようとする者があらかじめ許可された者であるかどうかを判定する個人識別装置1403を設置する。個人識別装置1403には，オフィス1400に入場しようとする者の顔画像を取得するカメラ104–1と指紋を取得する指紋入力装置105が接続される。さらに端末1408にログインしようとする者の顔画像を取得するカメラ104–2も接続される。

【００２６】図15は個人識別装置1403の機能構成の例である。図15において，図2の個人識別装置103と同じ番号を付している機能は同様に動作する。アクセス管理機能1515は，融合判定機能216の判定結果を受けて，アクセスログ202を更新し，アクセスを許可する。個人識別装置1503も，個人識別装置103と同様，図18に示すような一般的な計算機を用いて実現することができる。オフィス1400に入場しようとする者は，指紋入力装置105に指を置く。個人識別装置1403は指が指紋入力装置105に置かれたことを検知し，指紋画像を取得し，特徴量を抽出する。次に個人識別装置1403は抽出した特徴量をあらかじめ指紋特徴量データベース203に登録された個人毎の指紋の特徴量とを照合し，個人を特定する。指紋特徴量データベース203は図4に示すように入場を許可された者のID番号および指紋特徴量をあらかじめ記録している。さらに個人識別装置1403は，カメラ104–1から，入場しようとする者の顔画像を取り込み，顔の特徴量を抽出して顔特徴量データベース201に一時的に記録する。次に，入場しようとする者のIDおよび指紋の照合結果をアクセスログ202に記録して，ドア101を開錠する。入場した者が端末1408にログインする場合，個人識別装置1403は，カメラ104–2から入場者の顔画像を取得し，顔の特徴量を抽出する。個人識別装置1403は，端末1408のキーボードなどから入力され送信された個人IDから照合すべき者を特定し，カメラ104–2による顔画像と顔特徴量データベース201にあらかじめ記録された顔特徴量とを照合して類似度を得る。次に顔の類似度とアクセスログ202に記録された者の指紋の類似度とを用いて，融合判定により本人認証を行う。本人と認められる場合には端末1408に利用許可を送信する。端末1408はこれを受けて上記ログインしようとする者のログインを受け付ける。

【００２７】図16はオフィス1400への入場フローを例示する。

ステップ1605：指紋入力機能212が指紋入力装置105からオフィスに入場しようとする者の指紋画像を取り込む。

ステップ1610：指紋照合機能1514が，指紋特徴量データベース203にあらかじめ登録された，入場を許可された者の指紋特徴量とステップ1605で得た指紋画像を照合し，類似度を算出する。

ステップ1620：ステップ1610で得た類似度のうち最も大きい値があらかじめ定められたしきい値を越えていれば，個人を特定できたものとして次のステップに進む。それ以外は処理を終了する。

ステップ1625：顔画像入力機能211が，カメラ104–1から，オフィスに入場しようとする者の顔画像を取り込む。

ステップ1630：顔照合機能1513が，ステップ1625で得た顔画像から特徴量を抽出し，顔特徴量データベース201に記録する。顔特徴量データベース201には，ステップ1620で特定した個人IDと抽出した顔特徴量を，図3に示すように保存する。

ステップ1632：アクセス管理機能1515がステップ1620で入場を許可すると認めた者の個人IDおよび指紋照合の類似度をアクセスログ202に記録する。アクセスログ202は図6に示すように個人IDおよび照合の類似度などを持つ。

ステップ1635：アクセス管理機能1515がドア管理装置102に開錠命令を出す

ステップ1640：ドア管理装置102がドア101を開錠する。

【００２８】図17に端末1408を利用する時の処理フローを例示する。

ステップ1702：端末1408を使用しようとする者が個人IDを入力する。　ステップ1705：顔画像入力機能211がカメラ104–2から端末1408を使用しようとする者の顔画像を取り込み，特徴量を抽出する。

ステップ1710：顔照合機能1513が，顔特徴量データベース201に記録された者のうち，ステップ1702で入力された個人IDに対応する顔特徴量とステップ1705で抽出した顔画像の特徴量とを照合し，類似度を算出する。

ステップ1720：融合判定機能215が，ステップ1710で得た顔の類似度と，ステップ1632で，アクセスログ202に記録された個人IDの指紋の類似度を融合判定する。

ステップ1725：融合判定の評価値があらかじめ定めたしきい値よりも大きかった場合，融合判定機能215は，上記ログインしようとする者を利用資格を持つ者と認め，次のステップに進む。それ以外は処理を終了する。

ステップ1735：アクセス管理機能1515が端末1408に利用許可を送信する。　ステップ1737：端末1408が利用許可を受けてログインの受付処理を行う。

【００２９】本実施例においては，端末1408から入力される第2のアクセス（端末1408の使用）を行おうとする者の個人IDを選別に用いている。また，本実施例においては，第1のアクセス(ビル114への入場)時に，第2のアクセス(端末1408の使用)時の照合に用いる生体情報(顔特徴量)データベース201を作成しているが，第1の実施例における指紋特徴量データベース203と同様，生体情報(顔特徴量)データベース201をあらかじめ備えていても良い。上記実施例において，端末1408にログインする場合に，個人IDを入力しない方法も採用可能である。この場合はステップ1702を省略し，ステップ1710では顔特徴量データベース201に記録された全ての者との照合を行い，最も類似度の大きい者のID番号を採用すればよい。本実施例では，入場管理に指紋を，端末のログイン

13

管理に顔画像を用いているが，この限りではない。例えば第1の実施例と同じく，顔画像を用いるよりも高い判定精度が得られる指紋を，より高いセキュリティを必要とする端末のログイン管理に用いることも可能である。本実施例の指紋特徴量データベース203の代わりに，あらかじめ個人に，当該個人毎の指紋特徴量を記録したICカードを持たせておき，指紋特徴量を個人識別装置に読み込んで照合するようにしてもよい。上記各実施例においては，二重のアクセス制御を例示したが，三重以上のアクセス制御についても同様に行うことが可能である。また，内側のアクセス制御に，複数の，同じまたは異なるアクセス制御を並列に実施することも可能である。以上の実施例では，生体情報として，指紋，顔画像を例示した。生体情報はこれらに限定されず，その他，音声，掌形，掌紋，虹彩パターン，網膜パターン，耳形状，キーボード打鍵時の特徴(ログイン名やパスワードなど特定の単語を打ち込むときの，打鍵間隔，押下時間などのキーの打ち方)，におい，DNAなど，個人が持つ，あるいは発生する特有な情報を用いることも可能である。

【００３０】

【発明の効果】本発明によれば，アクセス管理システムが要求する本人確認の精度を満たし，かつ生体情報の偽造に対する高い耐性を持ち，なりすましによる不正なアクセスを防止できる。要求されるセキュリティレベルに応じた，適正なアクセス制御を行い，高い利便性，低いシステム構築コスト，短い計算時間を実現することができる。

【図面の簡単な説明】

【図１】第1の実施例の概略を説明する図である。

【図２】第1の実施例における個人識別装置の機能構成例を示す図である。

【図３】実施例における顔の特徴量データベース201の例である。

14

＊【図４】実施例における指紋特徴量データベースの例である。

【図５】実施例における判定基準データの例である。

【図６】実施例におけるアクセスログの例である。

【図７】実施例における本発明のビルへの入場管理の例を示すフロー図である。

【図８】実施例における本発明のコンピュータ室への入場管理の例を示すフロー図である。

【図９】実施例における判定機能に渡すデータの例である。

【図１０】実施例における融合判定の評価値の例である。

【図１１】第1の実施例における顔画像入力機能の機能構成例の図である。

【図１２】第1の実施例における輝度変換テーブルの例である。

【図１３】第1の実施例における顔の照合フローである。

【図１４】第2の実施例におけるオフィスへの入場管理の機能構成の例を示す図である。

【図１５】第2の実施例における個人識別装置の機能構成例を示す図である。

【図１６】第2の実施例におけるオフィスへの入場管理フローの例を示す図である。

【図１７】第2の実施例における端末へのログインのフローの例を示す図である。

【図１８】各実施例における個人識別装置を実現する計算機の概略構成図である。

【符号の説明】

100：コンピュータ室，101：外ドア，102：ドア管理装置，103：個人識別装置，104：カメラ，114：ビル，115：内ドア，202：アクセスログ，213：顔照合機能，214：指紋照合機能，216：融合判定機能。

＊

【図５】

図5

パラメータ	値
顔の類似度の係数	0.8
指紋の類似度の係数	1.2
融合判定のしきい値	12

【図６】

図6

個人ID	日時	照合の類似度
A001	99/2/22 15:00	8
A002	99/2/22 16:30	9
A010	99/2/22 17:10	7

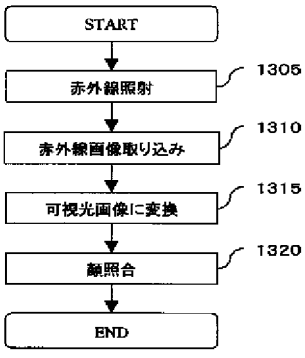
【図９】

図9

個人ID	顔照合の類似度	指紋照合の類似度
A001	8	1
A002	9	9

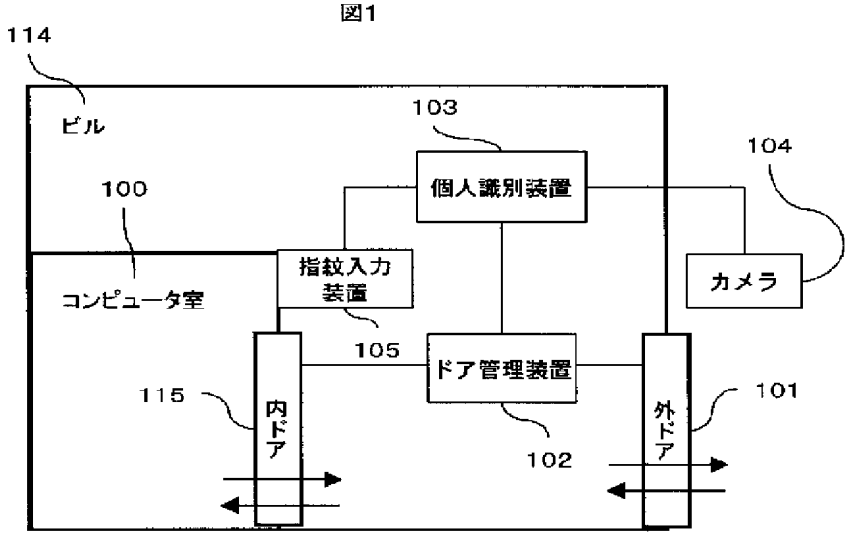
【図１３】

図13



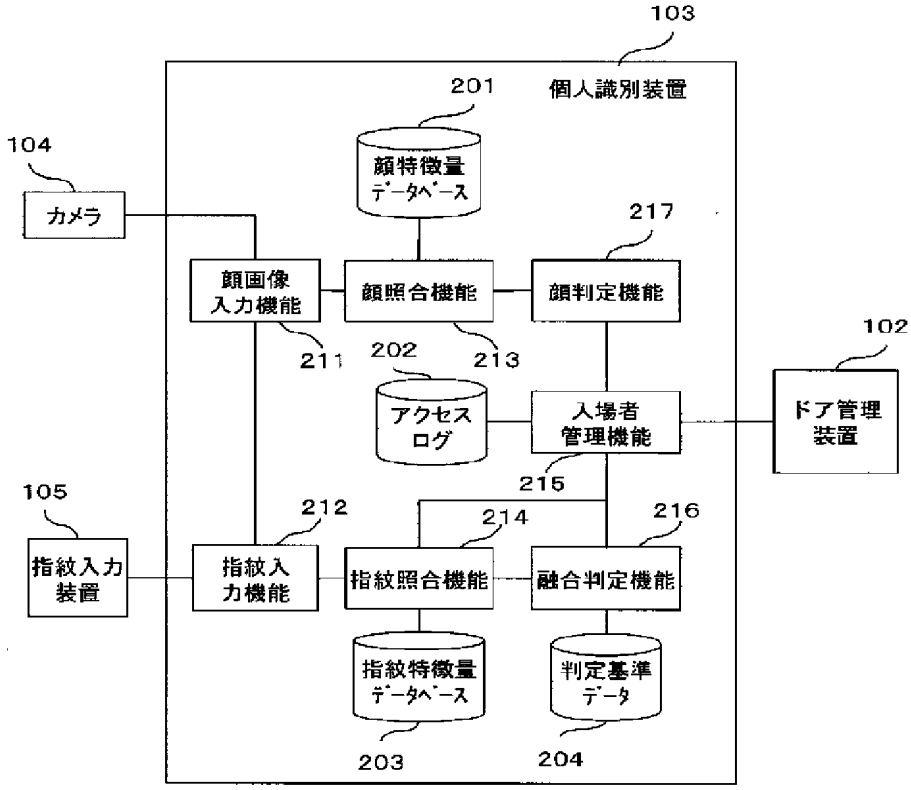
【図１】

図1


114
ビル
103
個人識別装置
104
100
コンピュータ室
指紋入力装置
カメラ
105
ドア管理装置
115
内ドア
外ドア
101
102

【図２】

図2


103
個人識別装置
201
顔特徴量データベース
104
カメラ
217
顔画像入力機能
顔照合機能
顔判定機能
211
213
202
102
アクセスログ
入場者管理機能
ドア管理装置
215
105
212
214
216
指紋入力装置
指紋入力機能
指紋照合機能
融合判定機能
指紋特徴量データベース
判定基準データ
203
204

【図３】

図3

個人ID	顔の特徴量
A001	**********
A002	**********
A003	**********
A004	**********
A005	**********
A006	**********
A007	**********
A008	**********
A009	**********
A010	**********

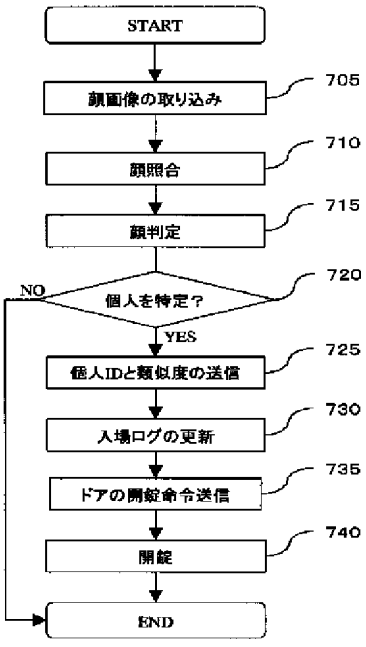
【図４】

図4

個人ID	指紋の特徴量
A001	**********
A002	**********
A003	**********
A004	**********
A005	**********
A006	**********
A007	**********

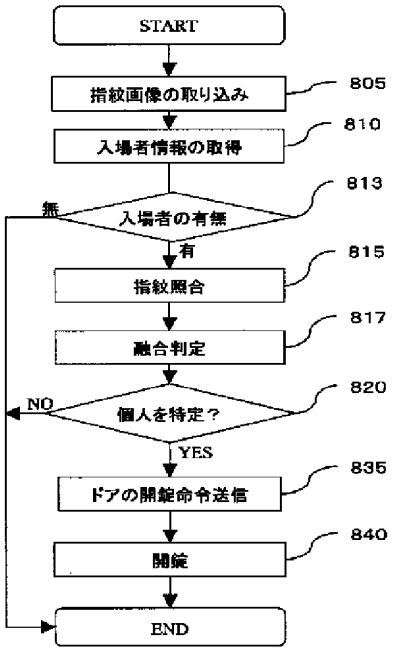
【図７】

図7



【図８】

図8



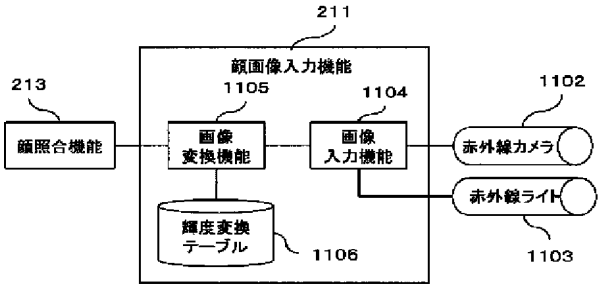
【図１０】

図10

個人ID	顔照合の類似度	指紋照合の類似度	評価値
A001	8	1	7.6
A002	9	9	18

【図１１】

図11



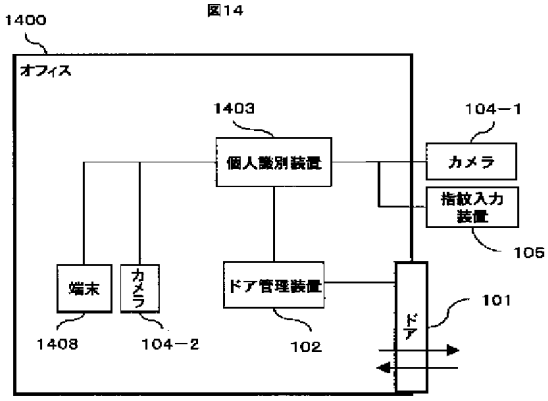
【図１２】

図12

赤外線画像の輝度	可視光画像の輝度
0	0
1	1
2	3
253	254
254	255
255	255

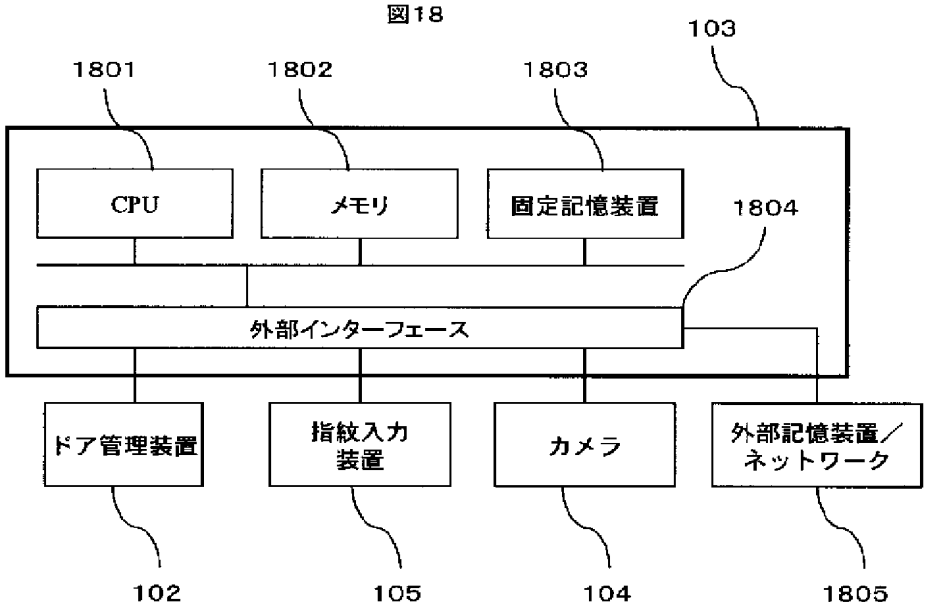
【図１４】

図14



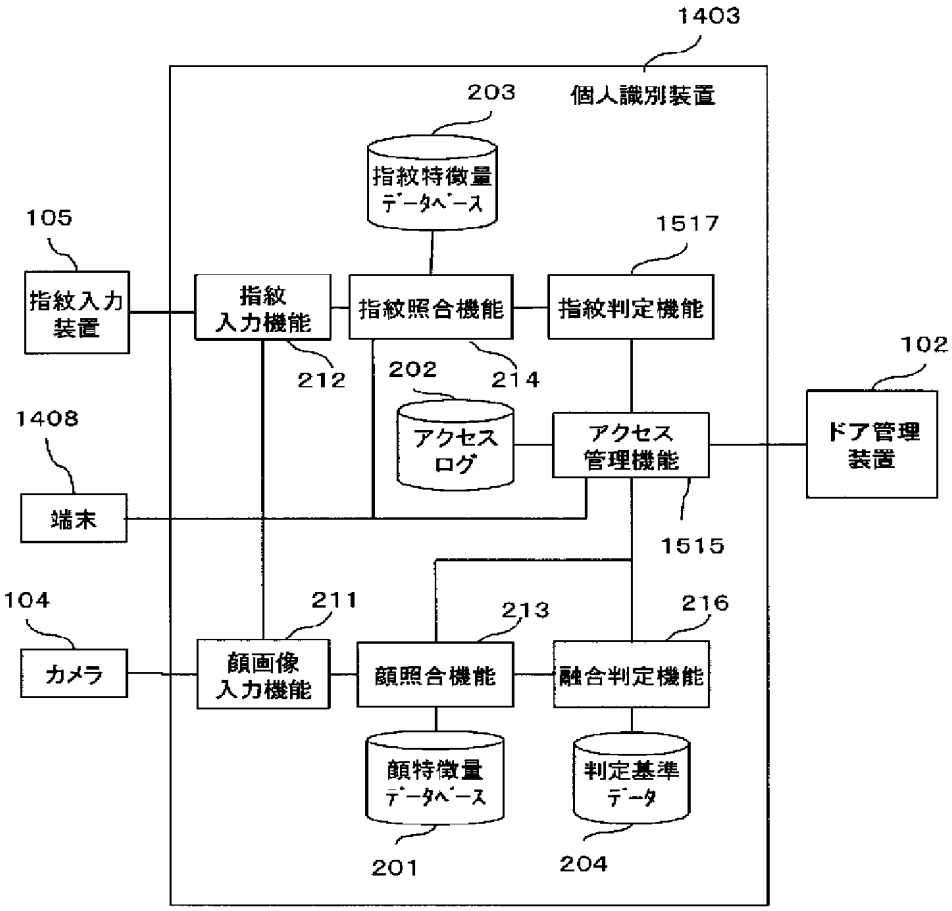
【図１８】

図18



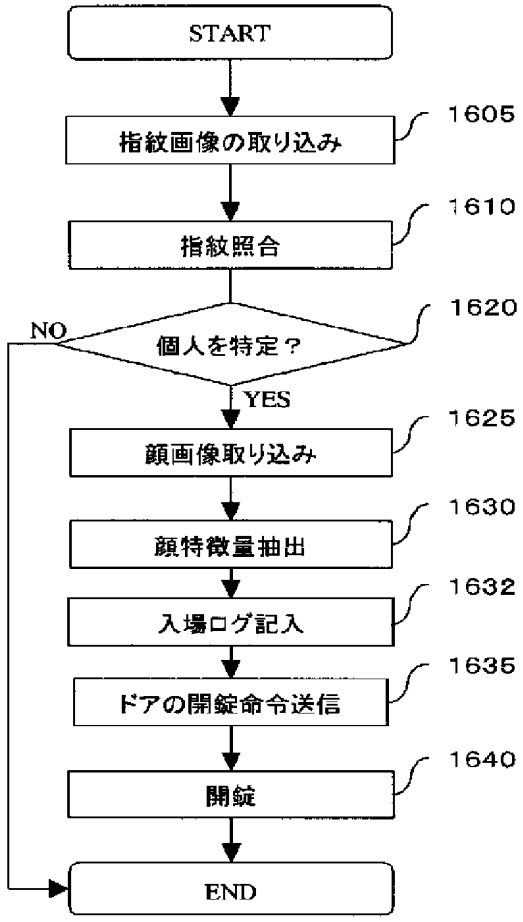
【図１５】

図15


1403
個人識別装置
203
指紋特徴量データベース
105
指紋入力装置
指紋入力機能
指紋照合機能
指紋判定機能
1517
212
214
202
102
アクセスログ
アクセス管理機能
ドア管理装置
1408
端末
1515
104
211
213
216
カメラ
顔画像入力機能
顔照合機能
融合判定機能
顔特徴量データベース
判定基準データ
201
204

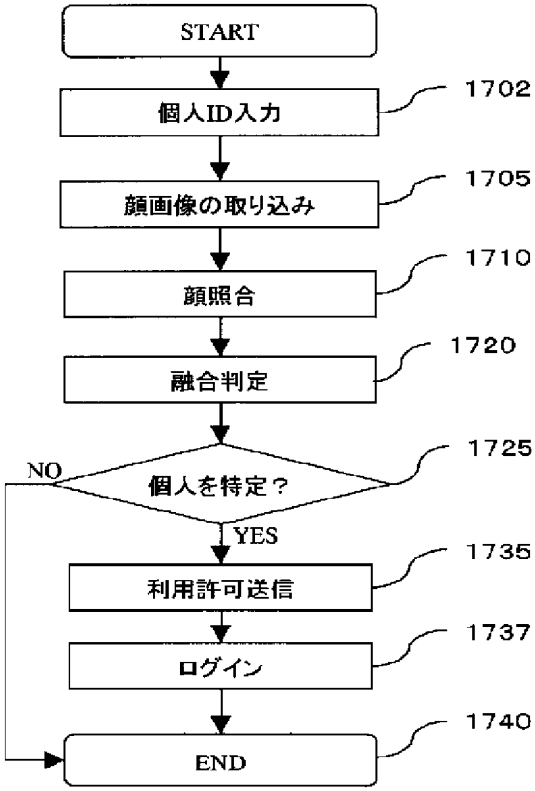
【図１６】

図16



【図１７】

図17



フロントページの続き

(72)発明者　村田　一吉
神奈川県横浜市戸塚区戸塚町216番地　株式会社日立製作所通信・社会システムグループ内

Ｆターム(参考)　2E250 AA03 AA04 AA12 BB05 BB30 BB47 CC13 DD08 DD09 DD10 EE03 EE15 FF08 FF11 FF18 GG05 GG15
5B043 AA09 BA02 BA04 FA07 FA09 GA01 GA13
5C087 BB03 DD06 DD23 DD43 EE08 FF01 FF04 FF19 GG02 GG10 GG19 GG59